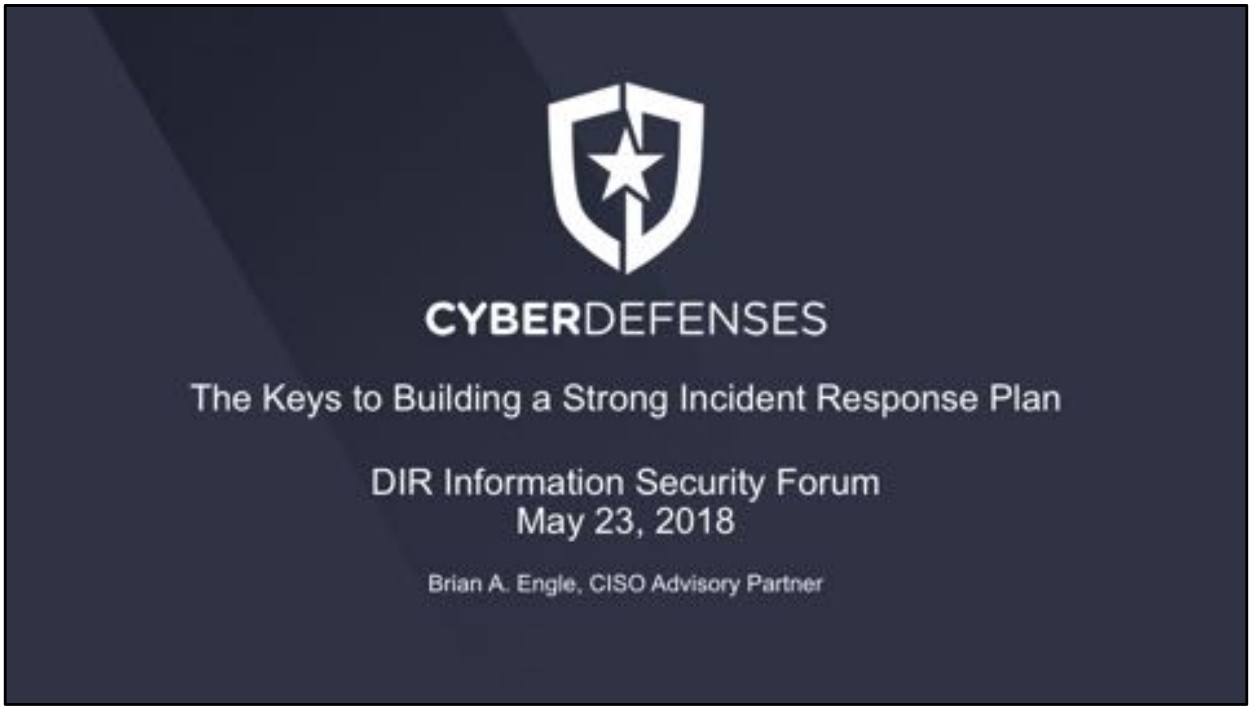


CYBERDEFENSES

The Keys to Building a Strong Incident Response Plan

DIR Information Security Forum
May 23, 2018

Brian A. Engle, CISO Advisory Partner

The Keys to Building a Strong Incident Response Plan

Session Overview

A Plan for Continuous Response

Essentials and the Stages of Response

Fighting Above Your Weight Class – Going From Good to Strong

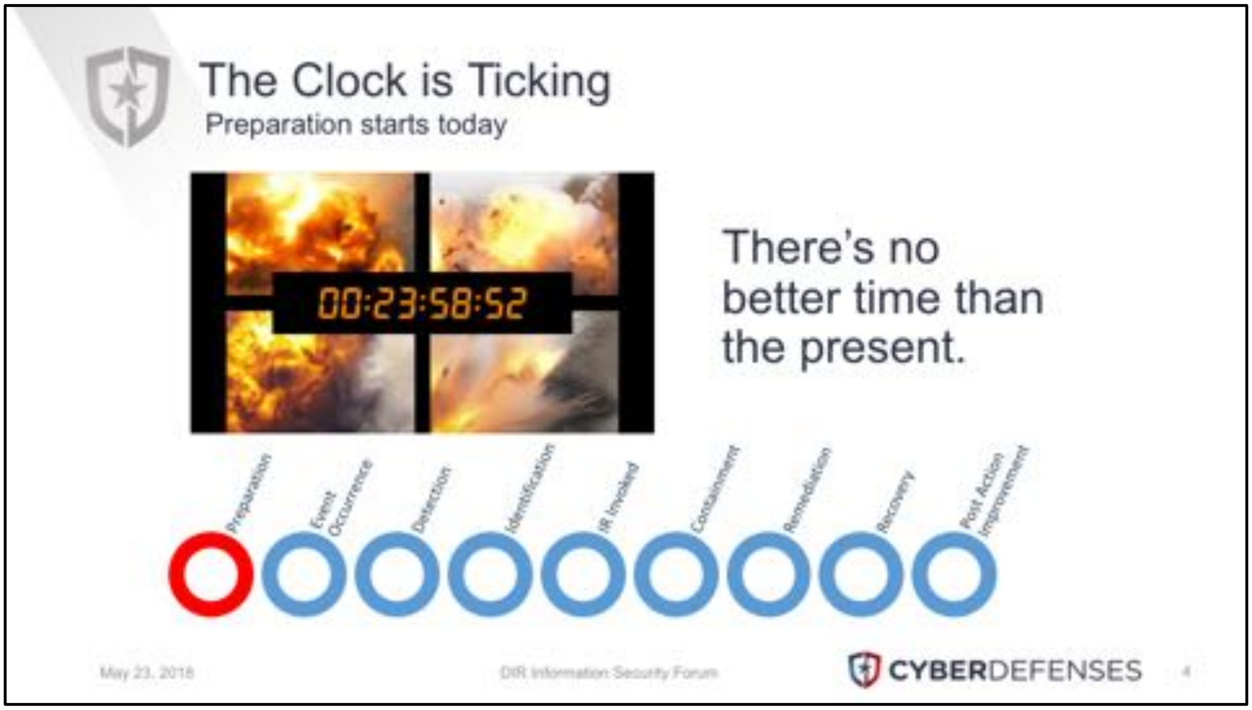
A Plan for Continuous Response

There's never a perfect time for things to go wrong…

CYBERDEFENSES

May 23, 2016

DIR Information Security Forum



The Clock is Ticking

Preparation starts today

There's no better time than the present.

Preparation

Event Occurrence

Detection

Identification

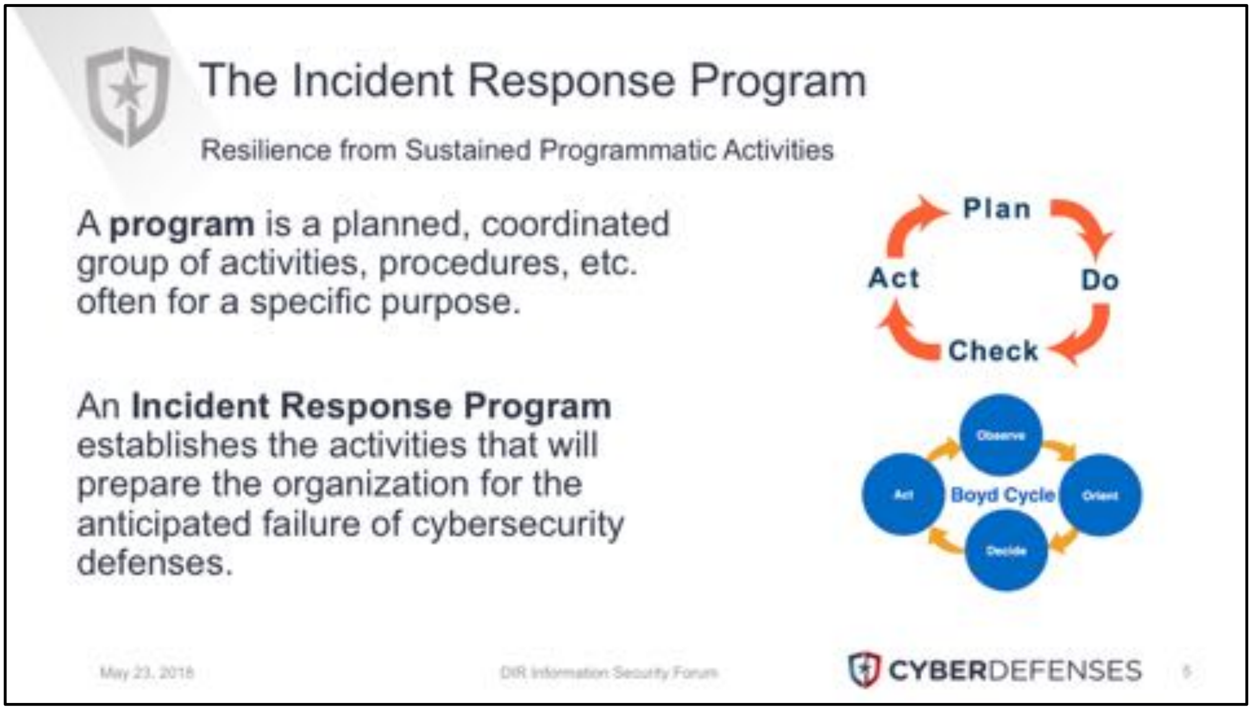
IR Invoked

Containment

Remediation

Recovery

Post Action Improvement



The Incident Response Program

Resilience from Sustained Programmatic Activities

A **program** is a planned, coordinated group of activities, procedures, etc. often for a specific purpose.

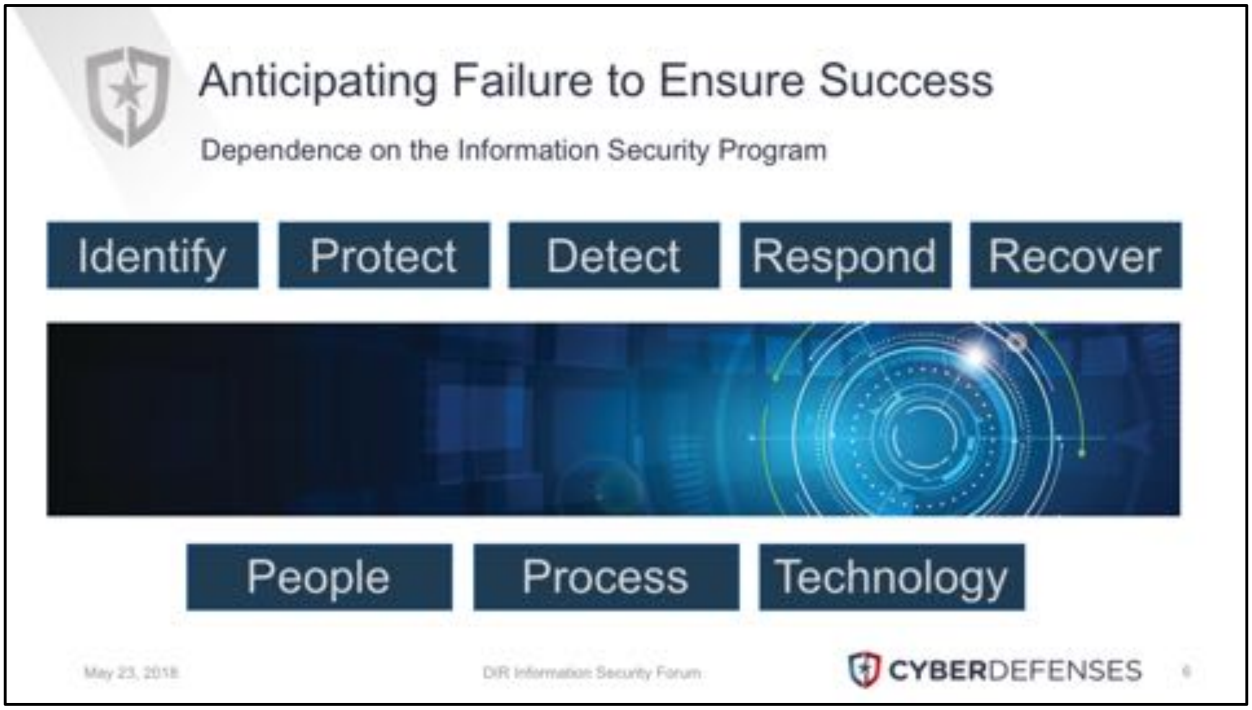
An **Incident Response Program** establishes the activities that will prepare the organization for the anticipated failure of cybersecurity defenses.

May 23, 2018

DIR Information Security Forum

CYBERDEFENSES

5



Anticipating Failure to Ensure Success

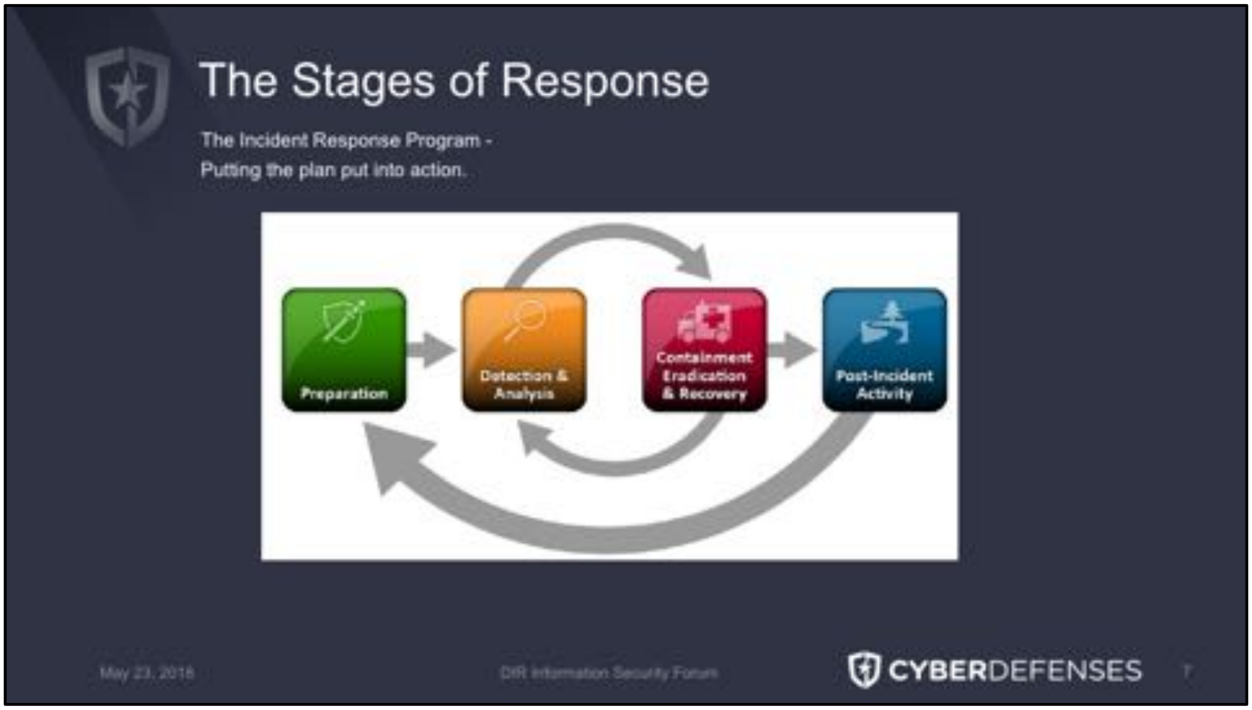
Dependence on the Information Security Program

Identify | Protect | Detect | Respond | Recover

People | Process | Technology

May 23, 2018 DIR Information Security Forum CYBERDEFENSES 6

Security Program elements. Traditional emphasis on protect (with prevent mentality). Not much attention on identify, detect, respond and recover.



The Stages of Response

The Incident Response Program -
Putting the plan put into action.

May 23, 2016 DIR Information Security Forum CYBERDEFENSES 7

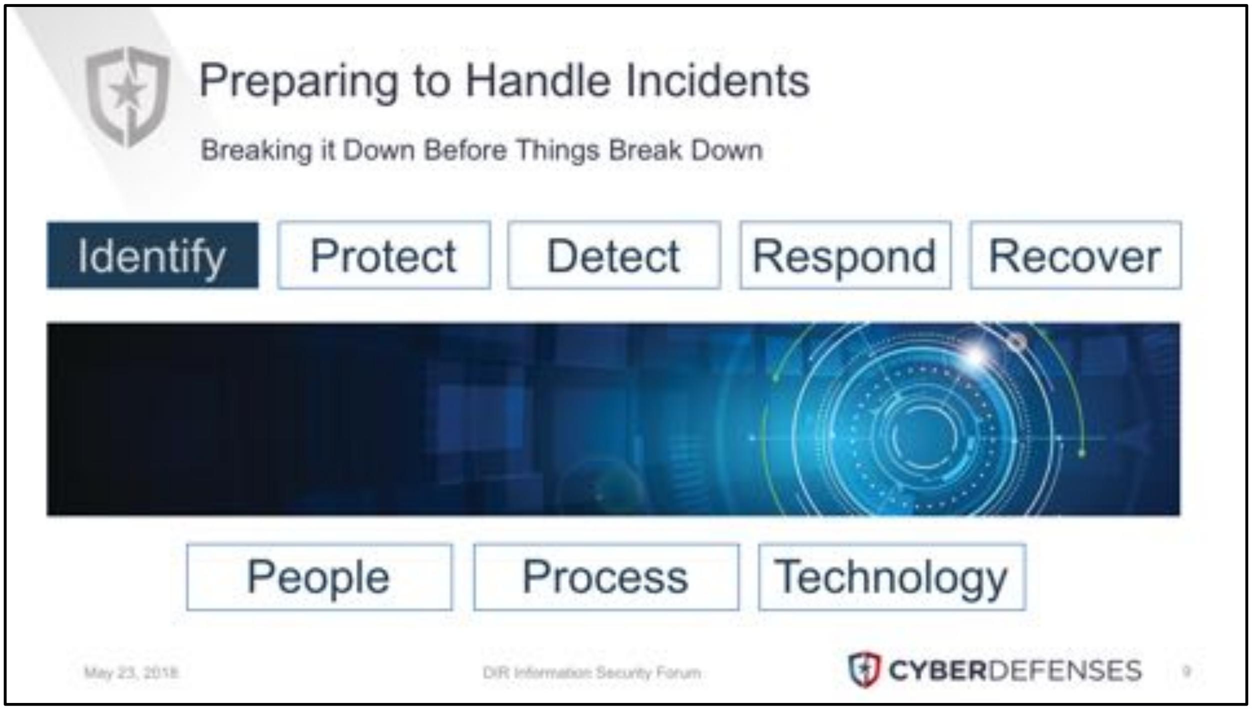
Preparation Stage

Fortune favors the prepared.

CYBERDEFENSES

May 23, 2018

DIR Information Security Forum



Preparing to Handle Incidents

Breaking it Down Before Things Break Down

Identify | Protect | Detect | Respond | Recover

People | Process | Technology

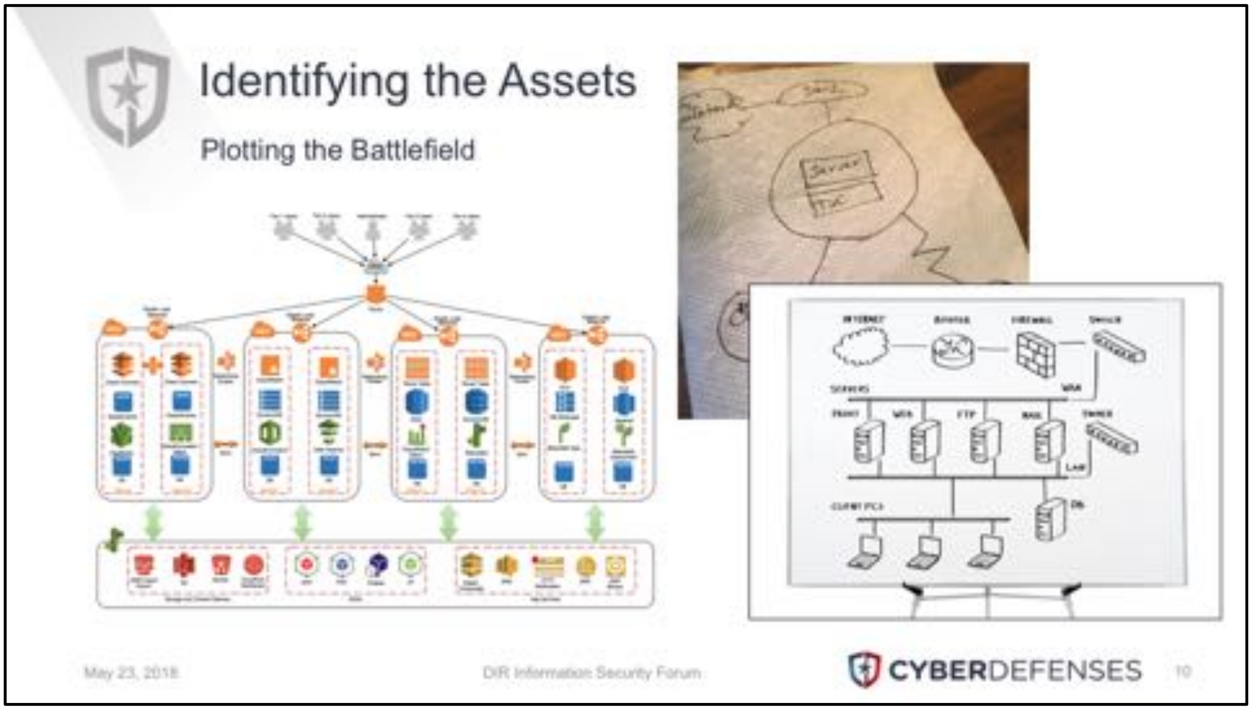
May 23, 2018 DIR Information Security Forum CYBERDEFENSES 9

Preparing to handle incidents

Identify the assets you are protecting

- Helps set priorities
- Puts resources towards the most important things
- When you’re in the middle of an incident – drawing a circle around the key assets, data elements, and egress points will help you potentially limit impact

Participating in the Risk Assessment processes helps draw out the likelihood of potential events, and identify threat groups/actors that may target the organization



Identifying the Assets

Plotting the Battlefield

May 23, 2018

DIR Information Security Forum

CYBERDEFENSES

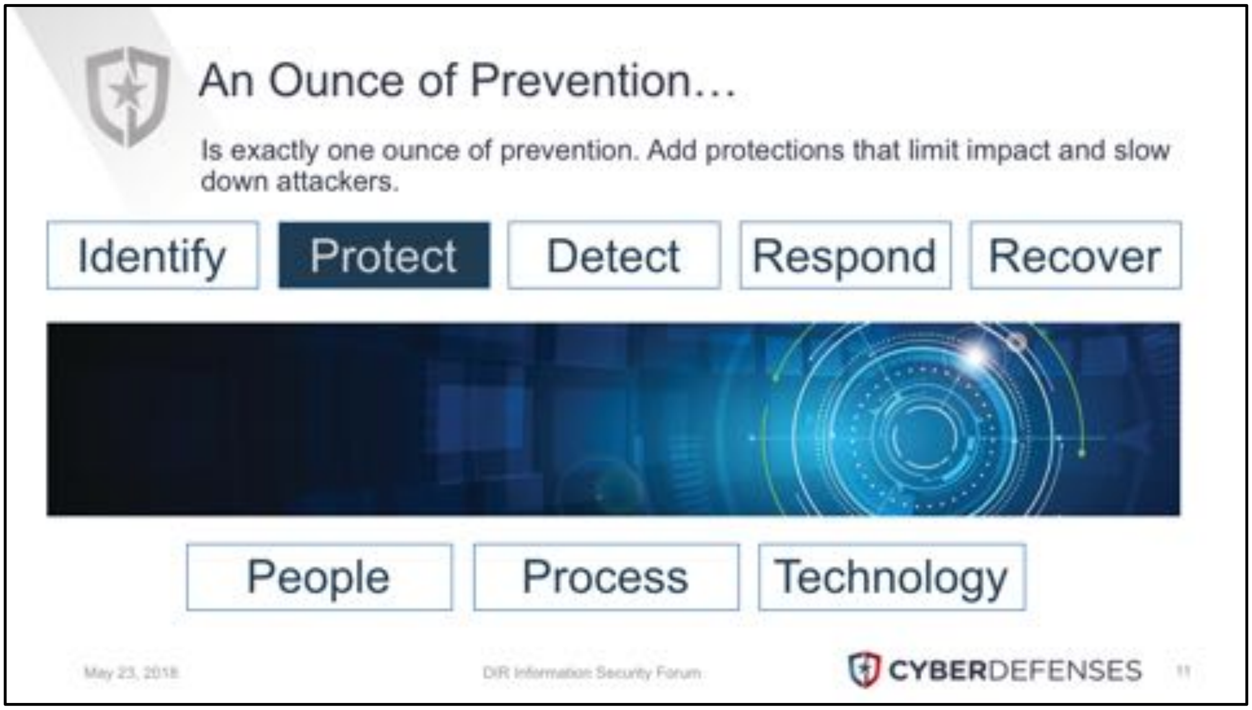
10

Everyone would love to have an updated, accurate network diagram to work off of.

What is more typical is a diagram that is developed on the spot.

It’s not the worst thing in the world to get the architecture up on the white-board of the war room, or incident command center.

Work with what you have.



An Ounce of Prevention…

Is exactly one ounce of prevention. Add protections that limit impact and slow down attackers.

Identify | **Protect** | Detect | Respond | Recover

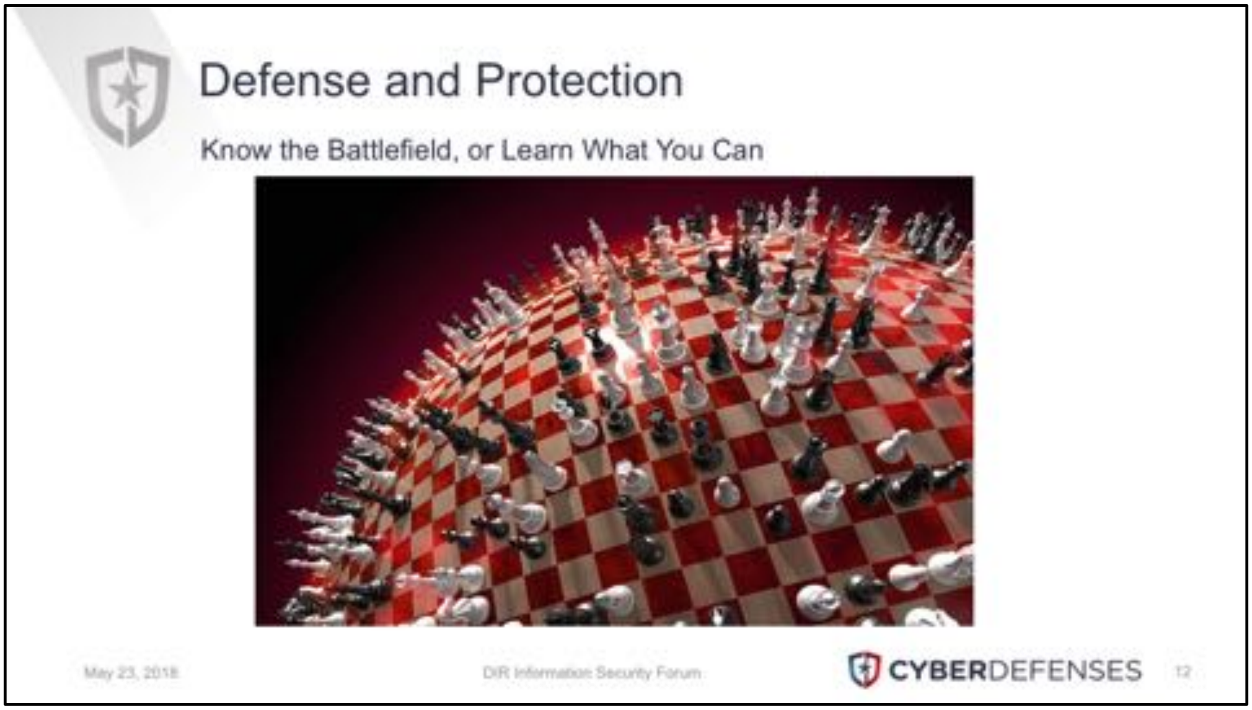
People | Process | Technology

May 23, 2018 DIR Information Security Forum CYBERDEFENSES 11

Preparing to handle incidents

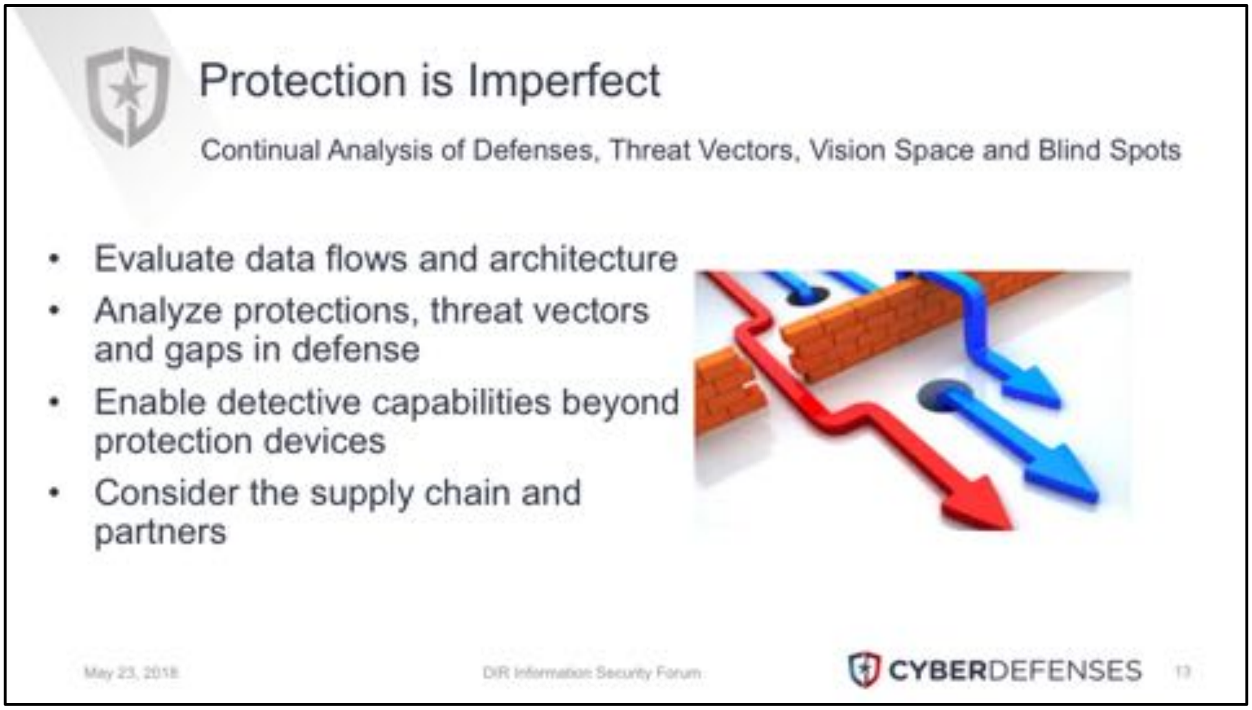
Understand where protections will prevent certain activities, limit others, or potentially slow down an attacker

- Compartmentalized networks, vs. flat networks



Defense and Protection

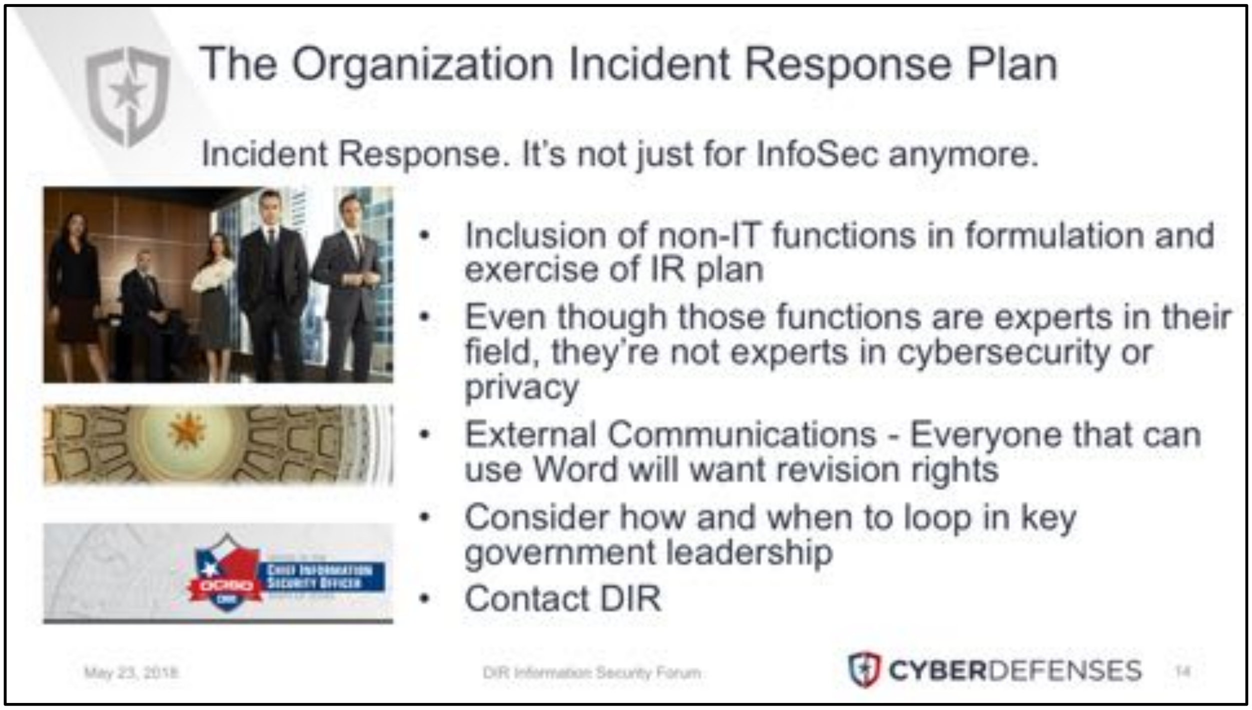
Know the Battlefield, or Learn What You Can



Protection is Imperfect

Continual Analysis of Defenses, Threat Vectors, Vision Space and Blind Spots

- Evaluate data flows and architecture
- Analyze protections, threat vectors and gaps in defense
- Enable detective capabilities beyond protection devices
- Consider the supply chain and partners



The Organization Incident Response Plan

Incident Response. It's not just for InfoSec anymore.

- Inclusion of non-IT functions in formulation and exercise of IR plan
- Even though those functions are experts in their field, they're not experts in cybersecurity or privacy
- External Communications - Everyone that can use Word will want revision rights
- Consider how and when to loop in key government leadership
- Contact DIR

Did Things Just Get Better…

Or worse

Legal Considerations for the Incident Response Plan

- Legal Team
- Privacy Officer
- Law Enforcement(s)

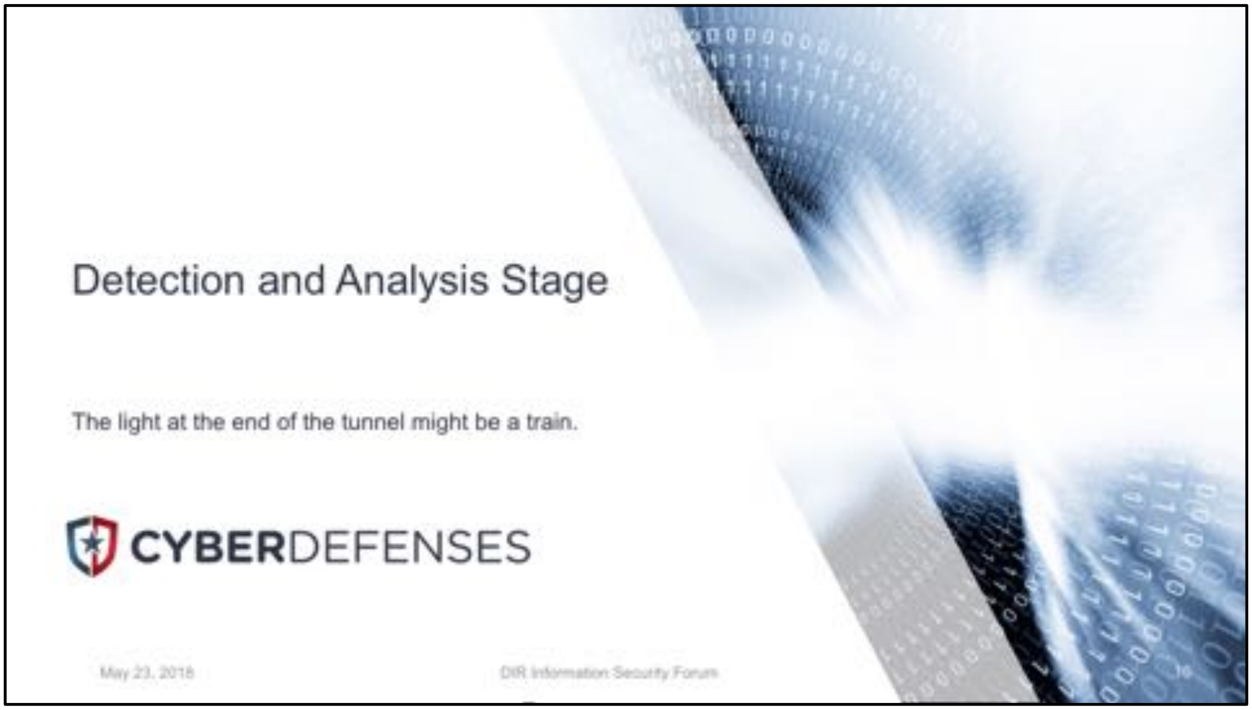
Litany of evidentiary concerns

- Who makes the call to Law Enforcement?
- When?
- Who has jurisdiction?
- Who will be most helpful?

Law Enforcement's goals are not always aligned with your goals

Texas Public CIO Academy – November 6, 2014

CYBERDEFENSES 15



Detection and Analysis Stage

The light at the end of the tunnel might be a train.

CYBERDEFENSES

There Are Two Types of Companies

"Look and you will find it – what is unsought will go undetected." - Sophocles

Identify | Protect | Detect | Respond | Recover

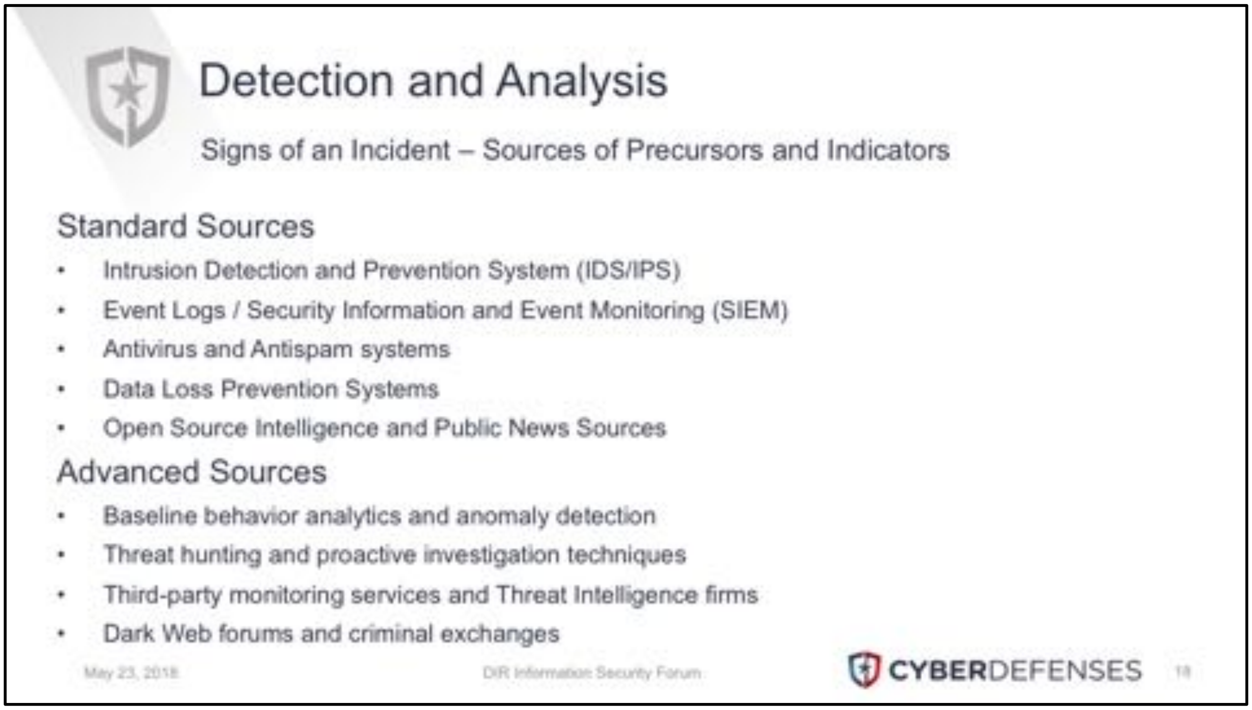
People | Process | Technology

May 23, 2018 DIR Information Security Forum CYBERDEFENSES 17

Know what you can see, understand blind spots.

Use intelligence and information sharing to improve visibility

IR and the SOC need to closely work together – in the development of processes, execution of ongoing monitoring and analysis, and certainly during the incident response process.



Detection and Analysis

Signs of an Incident – Sources of Precursors and Indicators

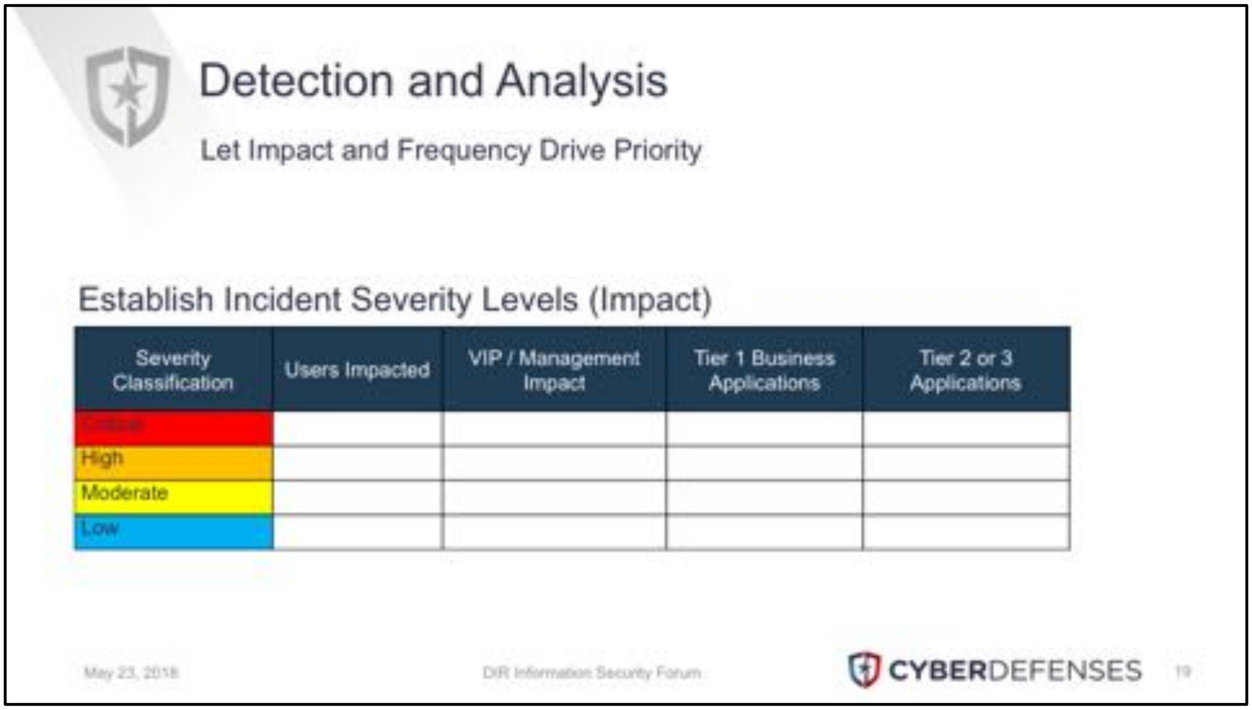
Standard Sources

- Intrusion Detection and Prevention System (IDS/IPS)
- Event Logs / Security Information and Event Monitoring (SIEM)
- Antivirus and Antispam systems
- Data Loss Prevention Systems
- Open Source Intelligence and Public News Sources

Advanced Sources

- Baseline behavior analytics and anomaly detection
- Threat hunting and proactive investigation techniques
- Third-party monitoring services and Threat Intelligence firms
- Dark Web forums and criminal exchanges

May 23, 2018 DIR Information Security Forum CYBERDEFENSES 18

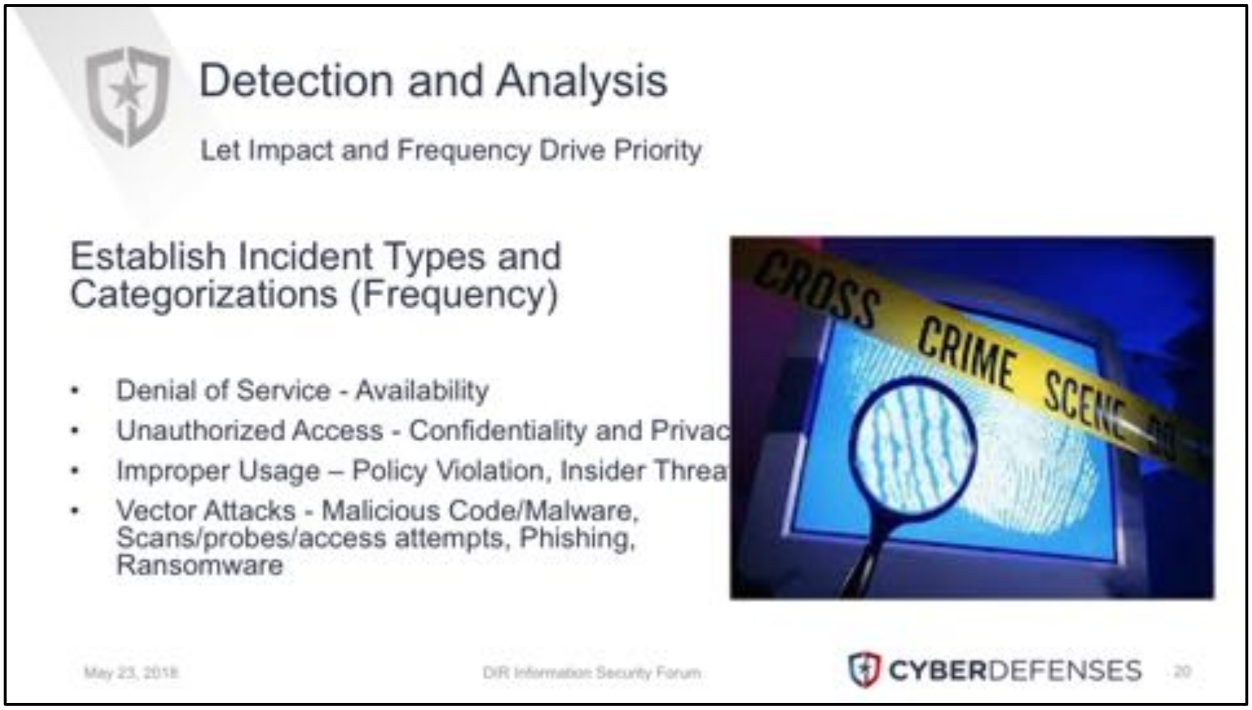


Detection and Analysis

Let Impact and Frequency Drive Priority

Establish Incident Severity Levels (Impact)

Severity Classification	Users Impacted	VIP / Management Impact	Tier 1 Business Applications	Tier 2 or 3 Applications
Critical				
High				
Moderate				
Low				



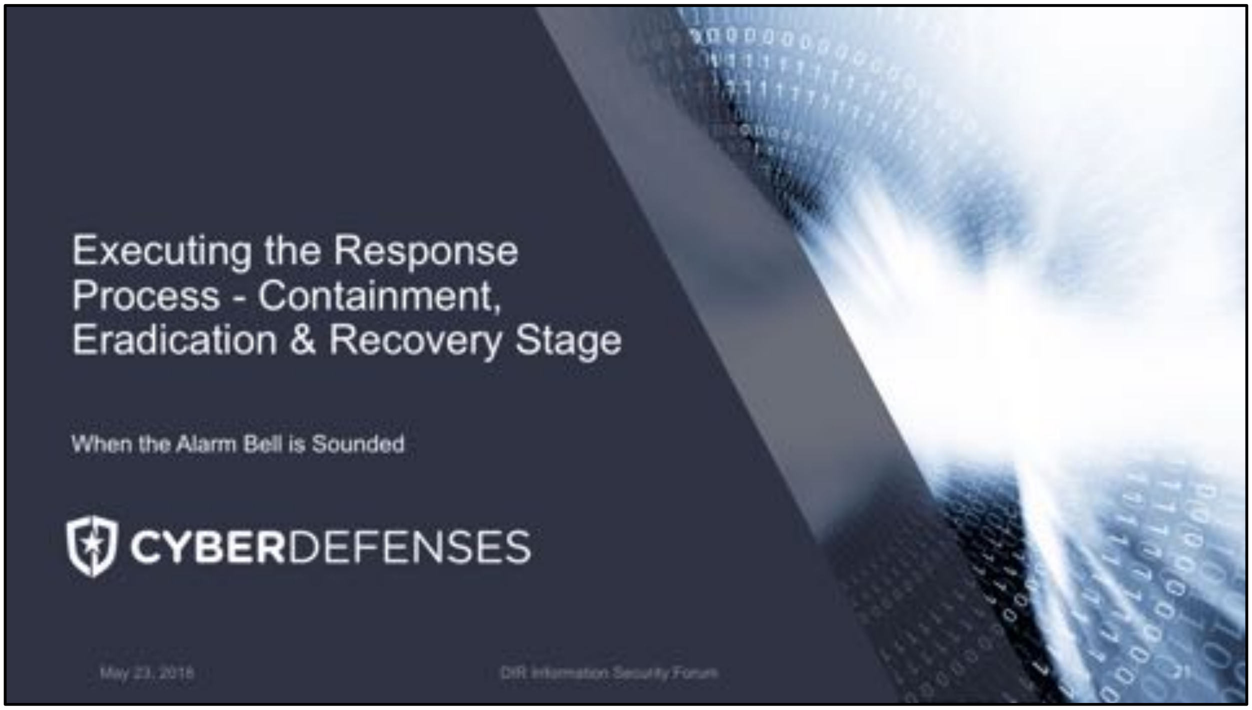
Detection and Analysis

Let Impact and Frequency Drive Priority

Establish Incident Types and Categorizations (Frequency)

- Denial of Service - Availability
- Unauthorized Access - Confidentiality and Privac
- Improper Usage – Policy Violation, Insider Threa
- Vector Attacks - Malicious Code/Malware, Scans/probes/access attempts, Phishing, Ransomware

CROSS CRIME SCENE DO



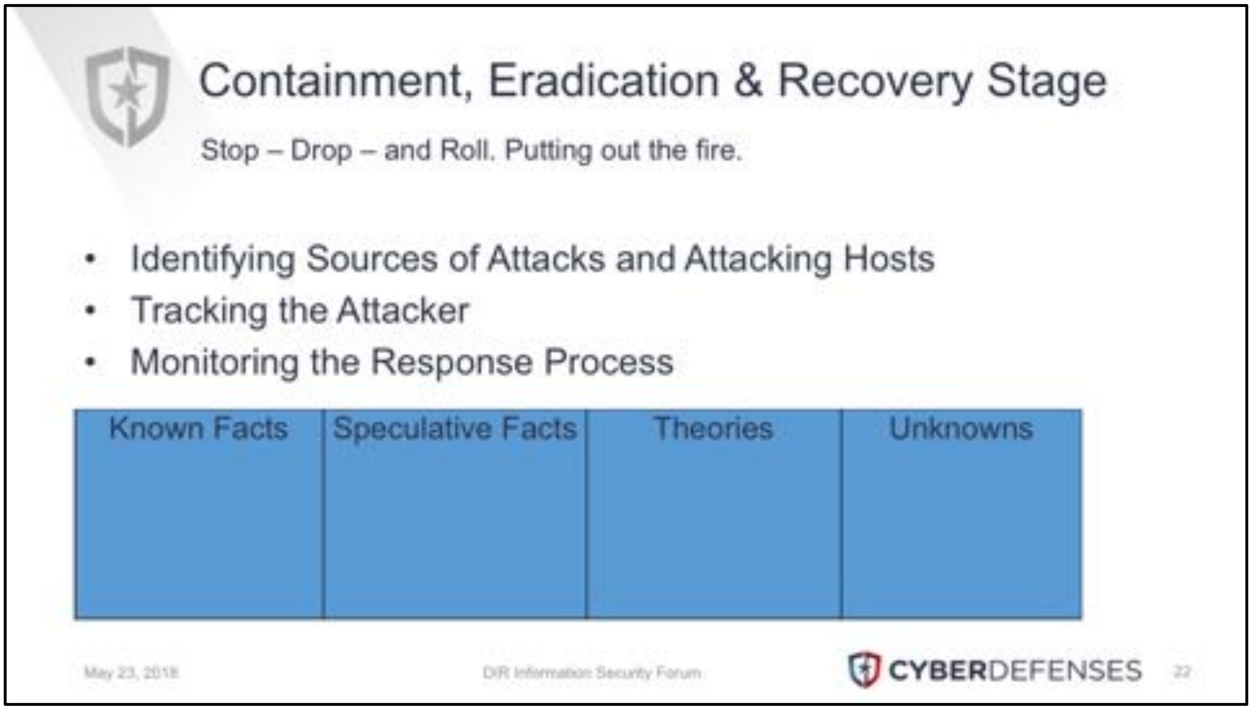
Executing the Response Process - Containment, Eradication & Recovery Stage

When the Alarm Bell is Sounded

CYBERDEFENSES

May 23, 2016

DIR Information Security Forum

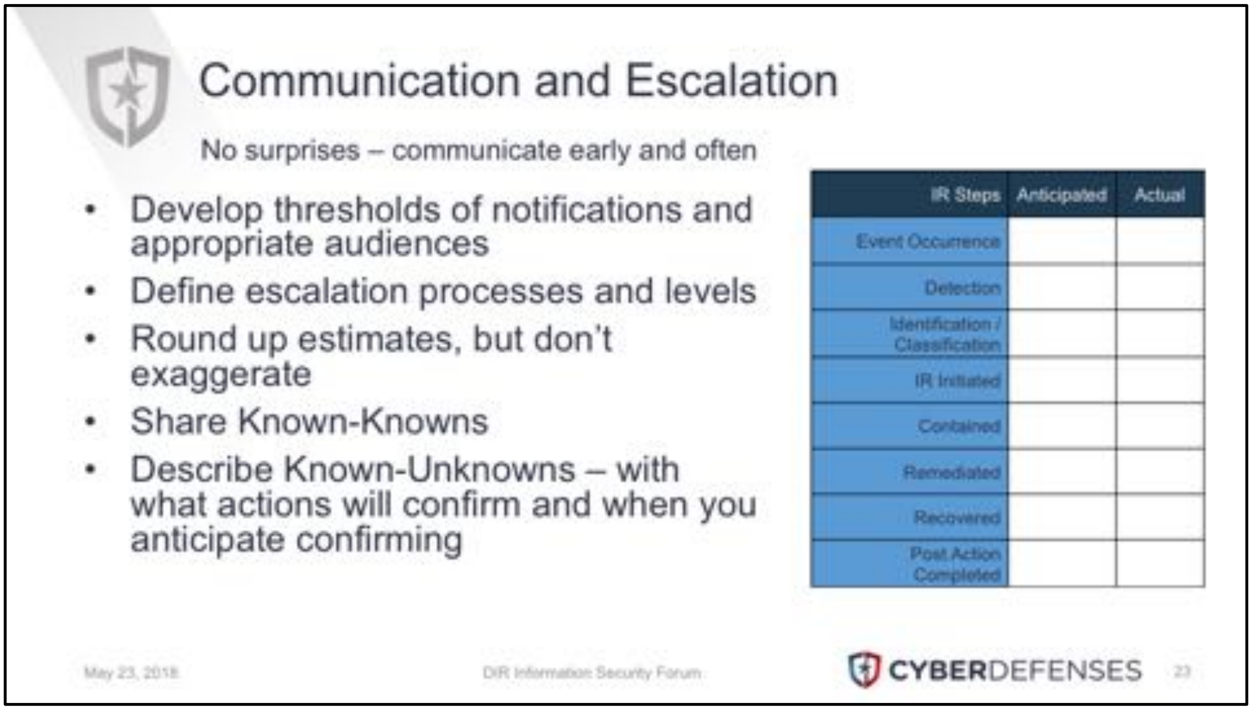


Containment, Eradication & Recovery Stage

Stop – Drop – and Roll. Putting out the fire.

- Identifying Sources of Attacks and Attacking Hosts
- Tracking the Attacker
- Monitoring the Response Process

Known Facts	Speculative Facts	Theories	Unknowns



Communication and Escalation

No surprises – communicate early and often

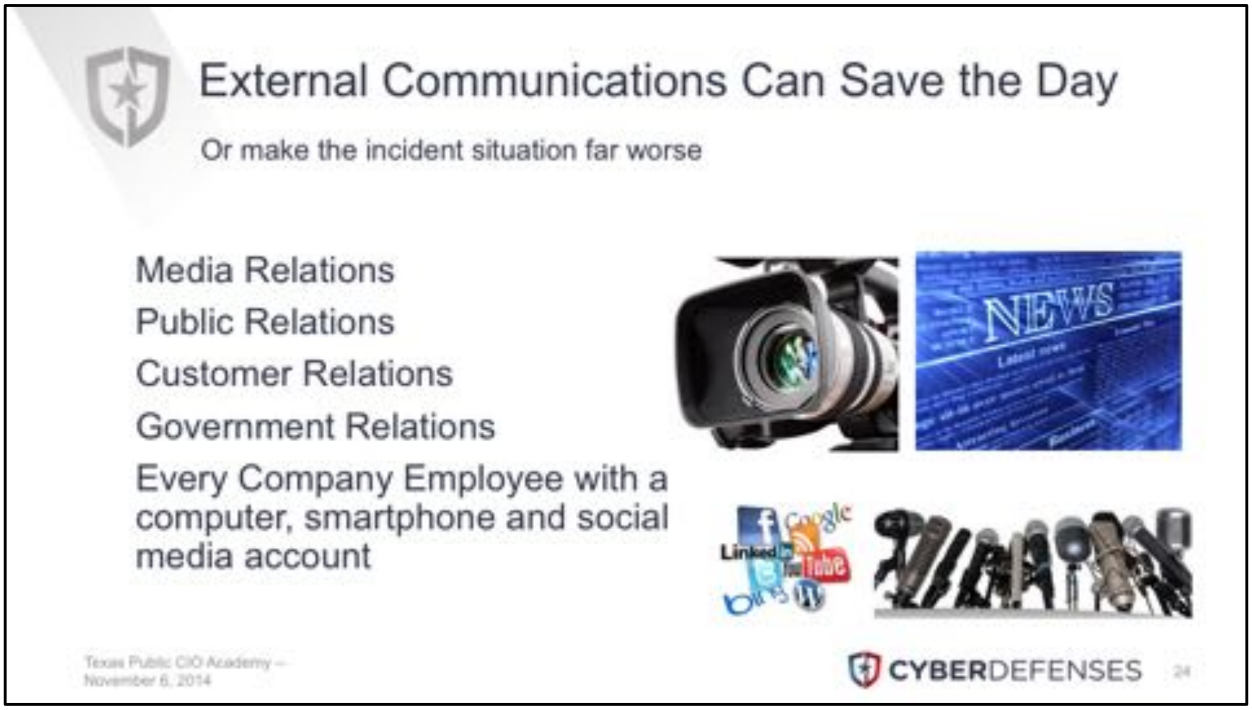
- Develop thresholds of notifications and appropriate audiences
- Define escalation processes and levels
- Round up estimates, but don't exaggerate
- Share Known-Knowns
- Describe Known-Unknowns – with what actions will confirm and when you anticipate confirming

IR Steps	Anticipated	Actual
Event Occurrence		
Detection		
Identification / Classification		
IR Initiated		
Contained		
Remediated		
Recovered		
Post Action Completed		

May 23, 2018 DIR Information Security Forum CYBERDEFENSES 23

In exercises, always round down, a lot.

In the real deal, round up, but only to the nearest whole number.



External Communications Can Save the Day

Or make the incident situation far worse

Media Relations

Public Relations

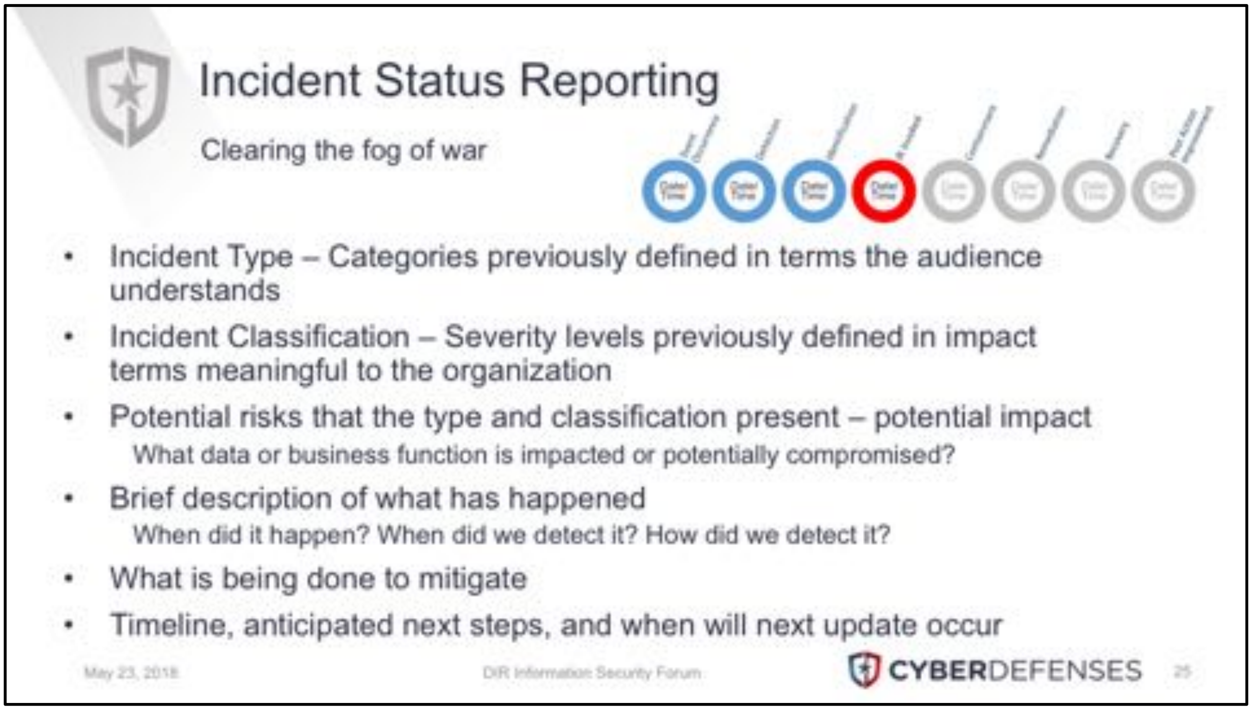
Customer Relations

Government Relations

Every Company Employee with a computer, smartphone and social media account

Texas Public CIO Academy – November 6, 2014

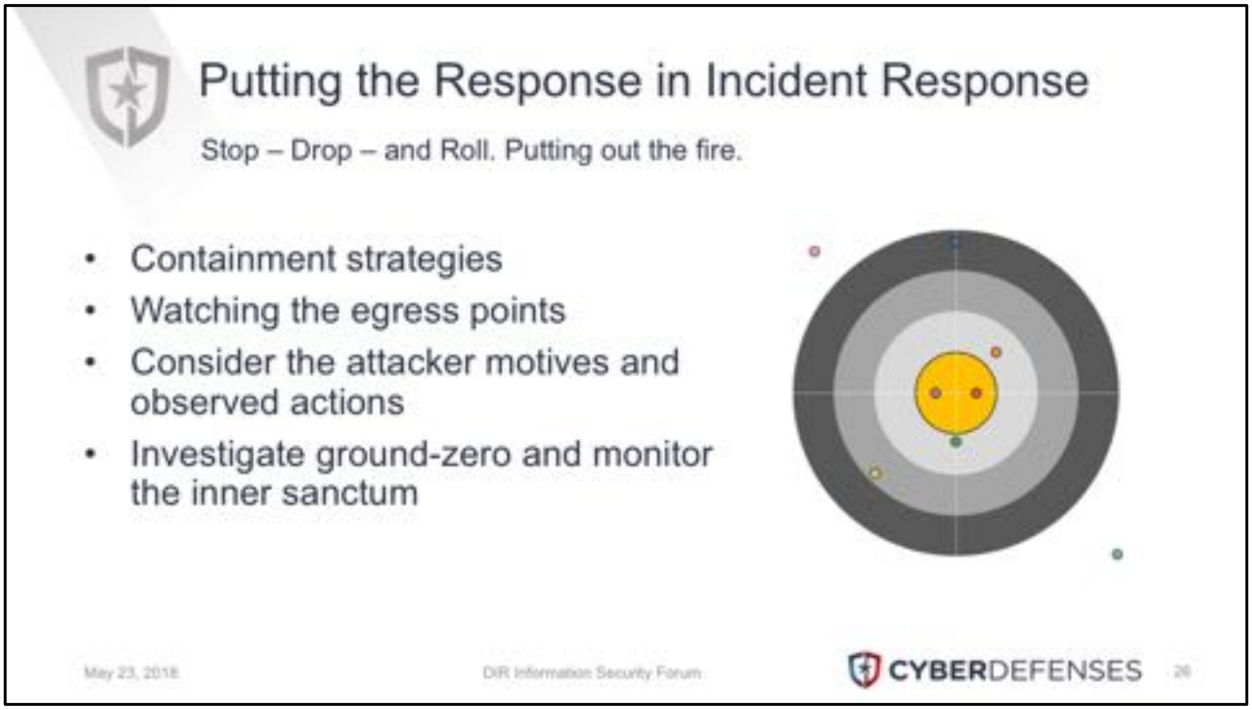
CYBERDEFENSES 24



Incident Status Reporting

Clearing the fog of war

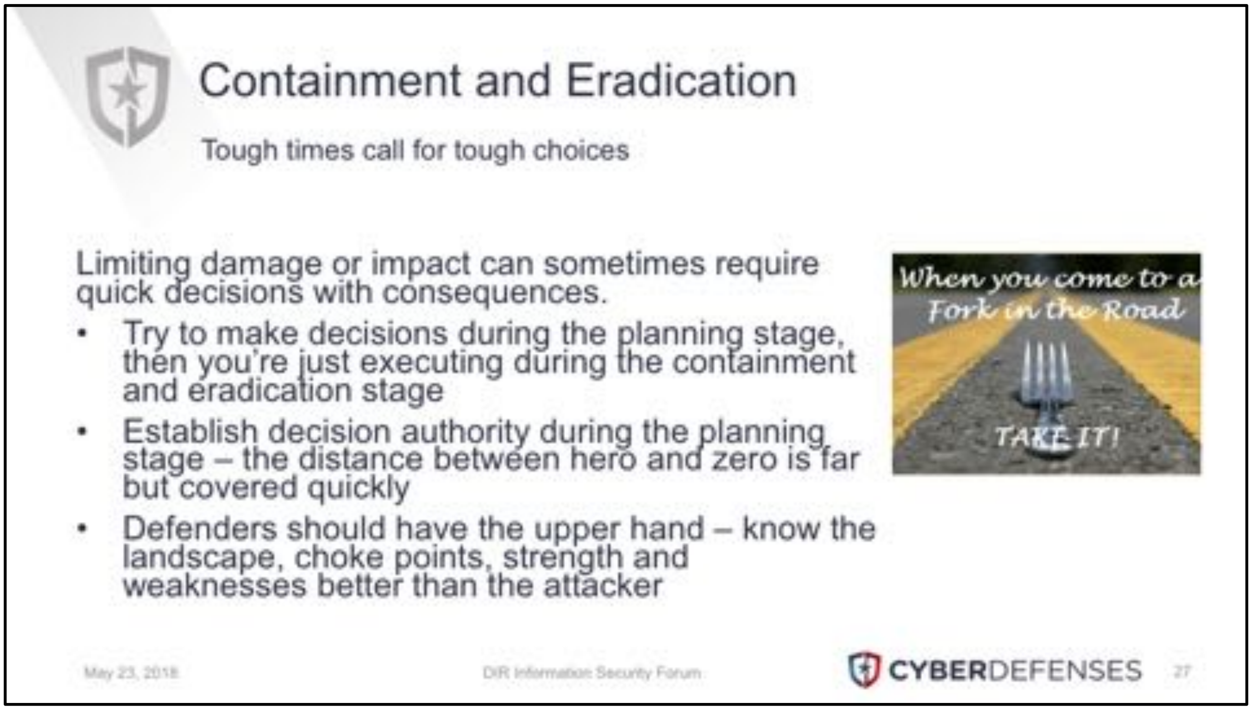
- Incident Type – Categories previously defined in terms the audience understands
- Incident Classification – Severity levels previously defined in impact terms meaningful to the organization
- Potential risks that the type and classification present – potential impact
  - What data or business function is impacted or potentially compromised?
- Brief description of what has happened
  - When did it happen? When did we detect it? How did we detect it?
- What is being done to mitigate
- Timeline, anticipated next steps, and when will next update occur



Putting the Response in Incident Response

Stop – Drop – and Roll. Putting out the fire.

- Containment strategies
- Watching the egress points
- Consider the attacker motives and observed actions
- Investigate ground-zero and monitor the inner sanctum



Containment and Eradication

Tough times call for tough choices

Limiting damage or impact can sometimes require quick decisions with consequences.

- Try to make decisions during the planning stage, then you're just executing during the containment and eradication stage
- Establish decision authority during the planning stage – the distance between hero and zero is far but covered quickly
- Defenders should have the upper hand – know the landscape, choke points, strength and weaknesses better than the attacker

May 23, 2018 DIR Information Security Forum CYBERDEFENSES 27

Post-Incident Activity Stage

At the end of the day is tomorrow.
Getting ready to do it all over again.

CYBERDEFENSES

May 23, 2018

DIR Information Security Forum

28

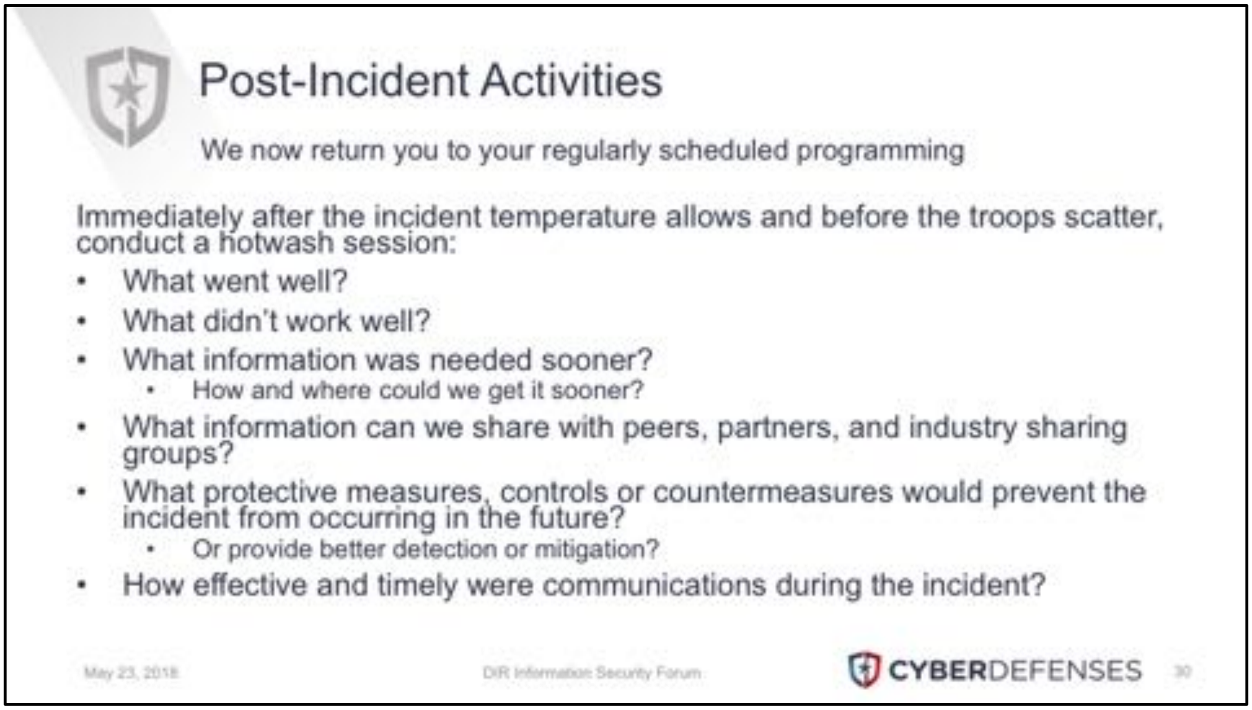
Post-Incident Activities

It's not just paperwork and reports - but start with completing the reporting with all of the data present

Gather data from the process:

- Time to detect
- Time to respond
- Time to contain
- Time to eradicate
- Time to remediate
- Time to full recovery
- Effort hours and costs

May 23, 2018 DIR Information Security Forum CYBERDEFENSES 29

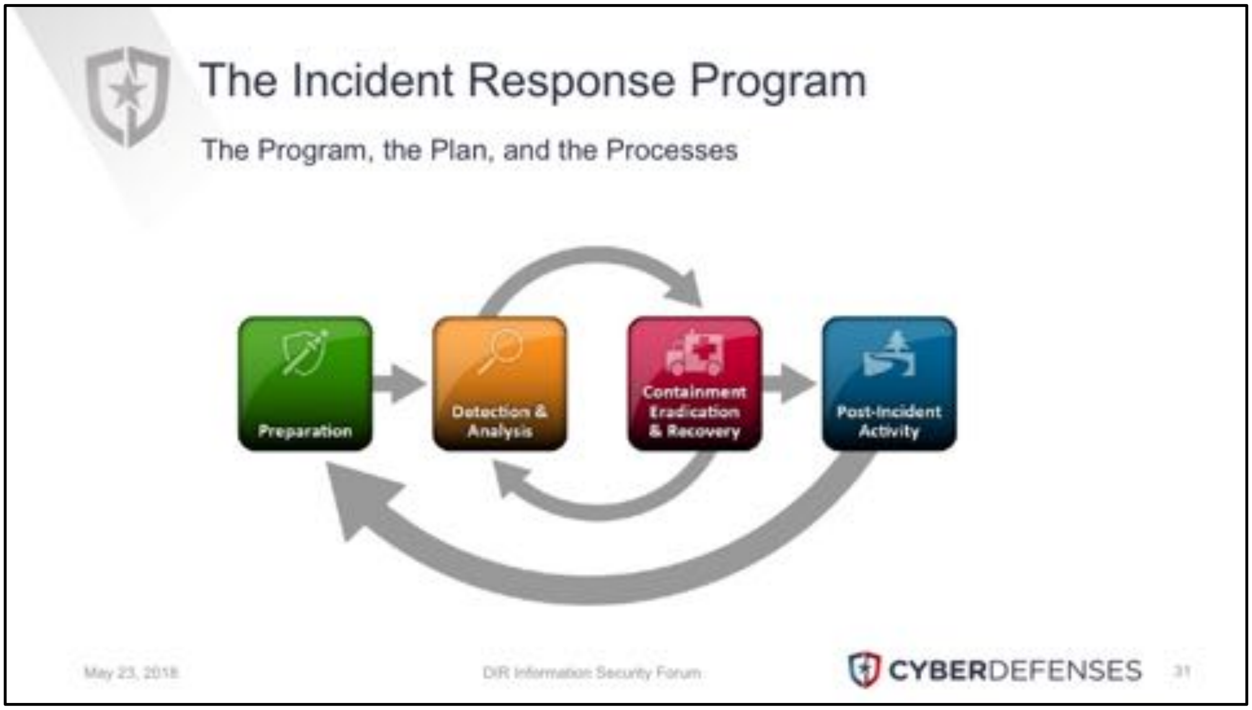


Post-Incident Activities

We now return you to your regularly scheduled programming

Immediately after the incident temperature allows and before the troops scatter, conduct a hotwash session:

- What went well?
- What didn't work well?
- What information was needed sooner?
  - How and where could we get it sooner?
- What information can we share with peers, partners, and industry sharing groups?
- What protective measures, controls or countermeasures would prevent the incident from occurring in the future?
  - Or provide better detection or mitigation?
- How effective and timely were communications during the incident?



The Incident Response Program

The Program, the Plan, and the Processes

Preparation

Detection & Analysis

Containment Eradication & Recovery

Post-Incident Activity

May 23, 2018

DIR Information Security Forum

CYBERDEFENSES 31

Fighting Above Your Weight Class

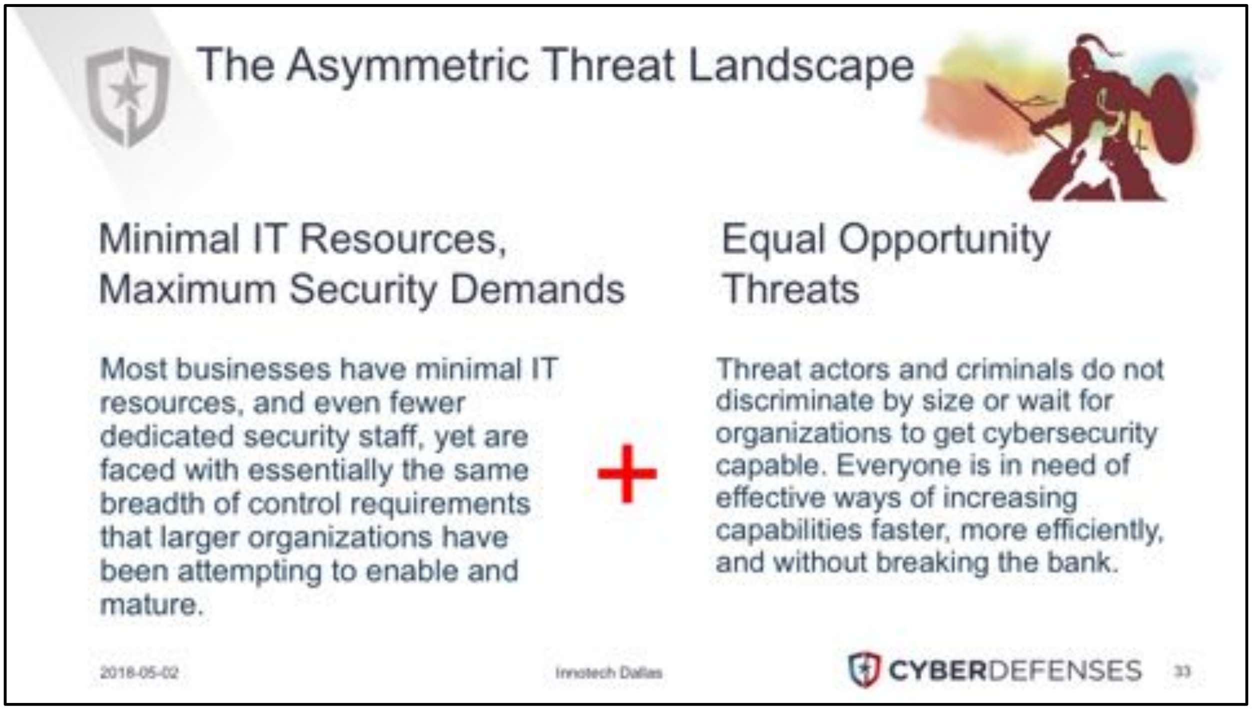
Going from good to strong.

CYBERDEFENSES

May 23, 2016

DIR Information Security Forum

32



The Asymmetric Threat Landscape

Minimal IT Resources, Maximum Security Demands

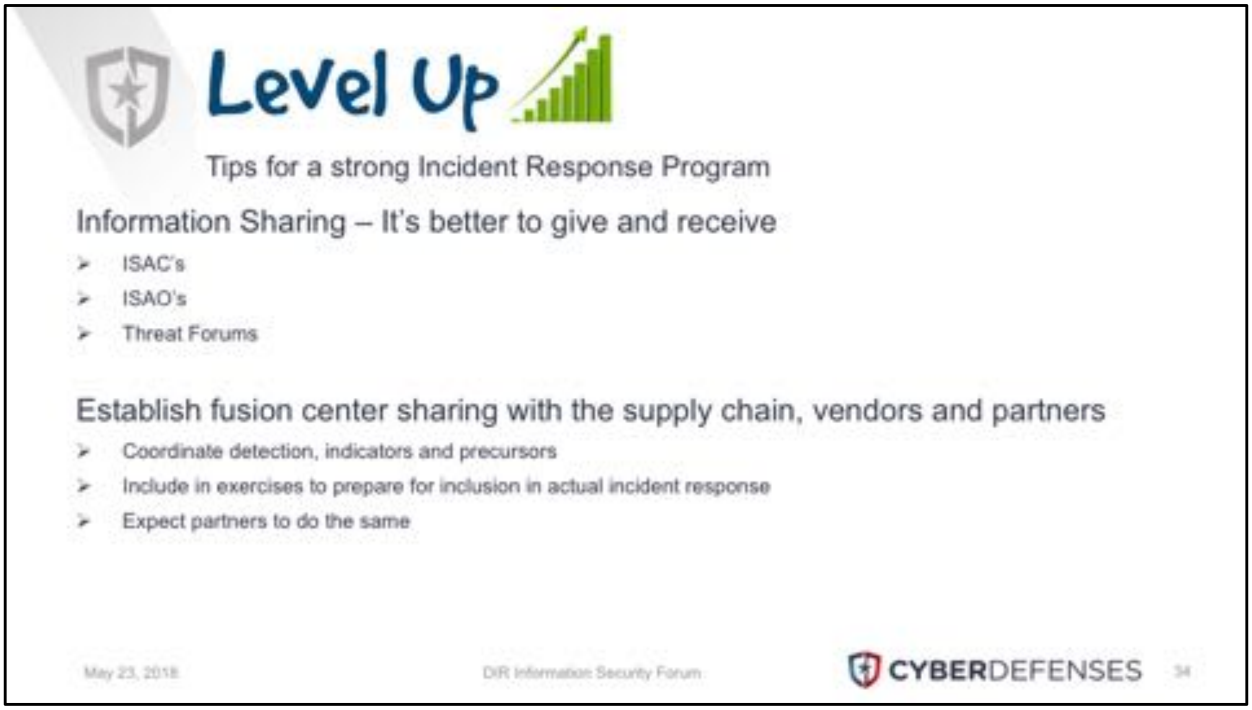
Most businesses have minimal IT resources, and even fewer dedicated security staff, yet are faced with essentially the same breadth of control requirements that larger organizations have been attempting to enable and mature.

+

Equal Opportunity Threats

Threat actors and criminals do not discriminate by size or wait for organizations to get cybersecurity capable. Everyone is in need of effective ways of increasing capabilities faster, more efficiently, and without breaking the bank.

2018-05-02 Innotech Dallas CYBERDEFENSES 33



Level Up

Tips for a strong Incident Response Program

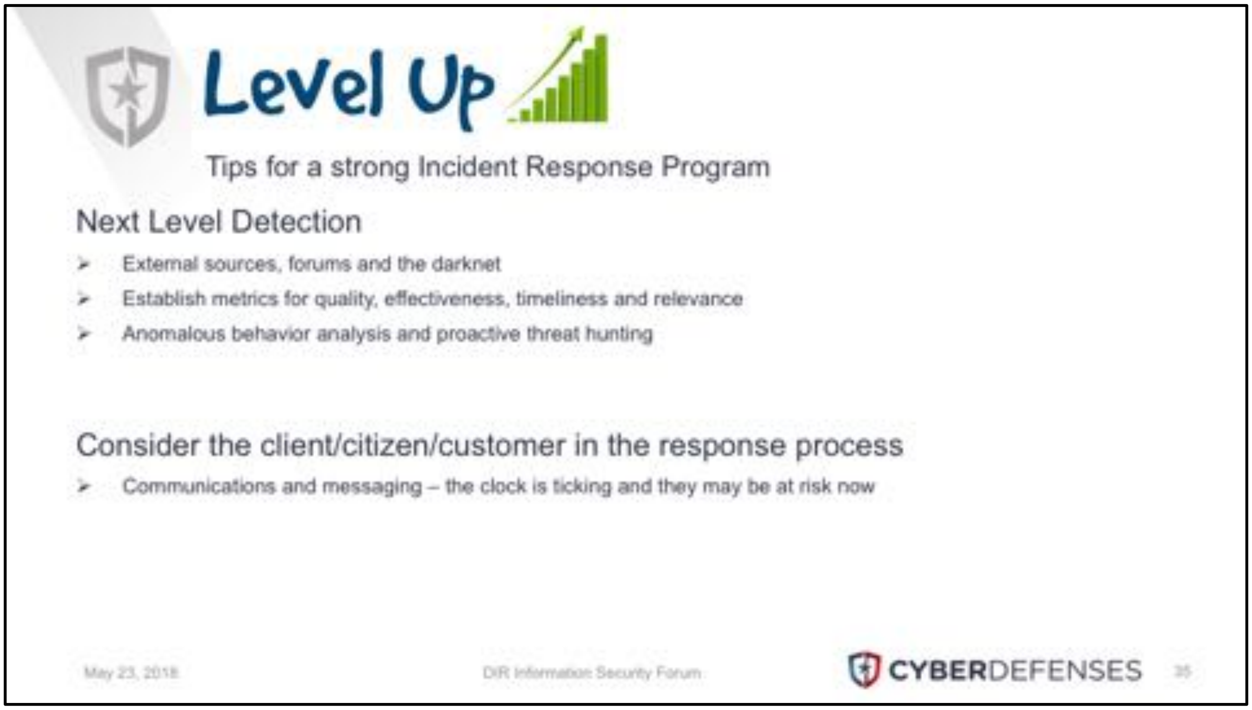
Information Sharing – It's better to give and receive

- ISAC's
- ISAO's
- Threat Forums

Establish fusion center sharing with the supply chain, vendors and partners

- Coordinate detection, indicators and precursors
- Include in exercises to prepare for inclusion in actual incident response
- Expect partners to do the same

May 23, 2018 DIR Information Security Forum CYBERDEFENSES 34



Level Up

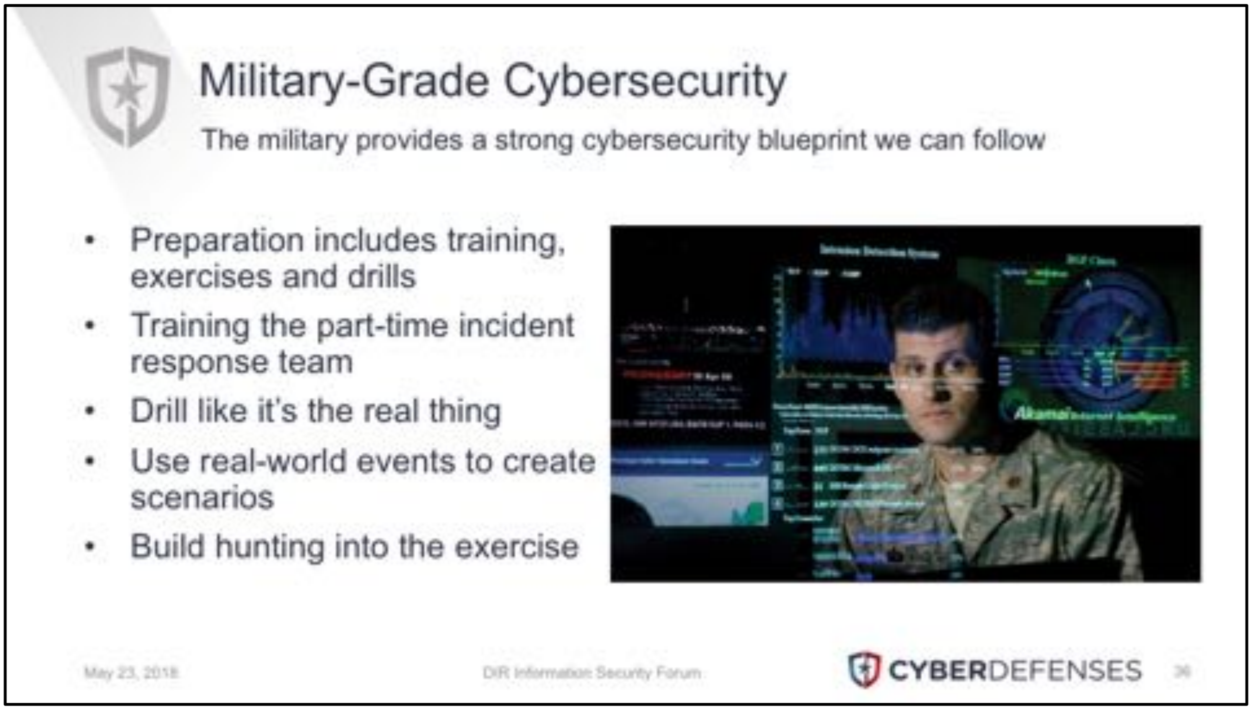
Tips for a strong Incident Response Program

Next Level Detection

- External sources, forums and the darknet
- Establish metrics for quality, effectiveness, timeliness and relevance
- Anomalous behavior analysis and proactive threat hunting

Consider the client/citizen/customer in the response process

- Communications and messaging – the clock is ticking and they may be at risk now



Intrusion Detection System
Akamai Internet Intelligence

Military-Grade Cybersecurity

The military provides a strong cybersecurity blueprint we can follow

- Preparation includes training, exercises and drills
- Training the part-time incident response team
- Drill like it's the real thing
- Use real-world events to create scenarios
- Build hunting into the exercise

May 23, 2018 DIR Information Security Forum CYBERDEFENSES 36

- Military Grade – level-headed calm under extreme conditions that preparedness achieves
- Executing to a plan prepared for anticipated or predicted likely event types – or adjusted as needed to adapt an overcome
- CyberDefenses has a military heritage that has been a key part of shaping our approach to cybersecurity

CYBERDEFENSES

THANK YOU

1205 Sam Bass Rd. Suite 300 Round Rock, TX 78681
512-255-3700 • info@cyberdefenses.com • www.cyberdefenses.com